Evento	Salão UFRGS 2018: SIC - XXX SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2018
Local	Campus do Vale - UFRGS
Título	Ferramenta Configurável de Proteção de Processadores Contra Falhas Transientes por Técnicas Baseadas em Software
Autor	EMANUEL TERIBELE NOVAKOSKI
Orientador	JOSÉ RODRIGO FURLANETTO DE AZAMBUJA

Ferramenta Configurável de Proteção de Processadores Contra Falhas Transientes por Técnicas Baseadas em Software

Aluno: Emanuel Novakoski
Orientador: José Rodrigo Azambuja
Universidade Federal do Rio Grande do Sul

I. Introdução

Processadores fabricados com transistores nanométricos operando em alta frequência são sensíveis a falhas produzidas pela colisão de partículas carregadas com o circuito. O efeito dessas colisões pode ser percebido nos programas por incoerências nos dados ou mudança no fluxo normal de execução do programa.

Existem várias técnicas para detectar e corrigir esses erros, divididas em técnicas baseadas em hardware e técnicas baseadas em software. Técnicas baseadas em hardware modificam a organização física do equipamento, levando a um aumento em área e consumo de energia, além de aumentar o custo de produção. Técnicas baseadas em software modificam apenas o código-fonte do programa, permitindo a aplicação das técnicas em processadores comerciais.

II. Ferramenta Proposta: CFT

A CFT é uma ferramenta configurável projetada para modificar o código em nível Assembly, o que reduz a complexidade de modificar o código de máquina e permite que os compiladores e montadores possam ser usados sem modificações.

A ferramenta é dividida em vários módulos, de acordo com sua função, descritos a seguir.

O primeiro módulo é o de configurações. Este é responsável por ler arquivos de configurações fornecidos pelo usuário, descrevendo a arquitetura do processador, bem como as modificações a serem aplicadas. Dessa forma a ferramenta se torna independente da arquitetura.

O segundo módulo é responsável pela formatação do código do programa. Inicialmente o módulo remove os espaços em branco e comentários do texto. Posteriormente o módulo analisa todos os recursos utilizados pelo programa e atribui recursos adicionais para aplicação das técnicas de proteção.

O terceiro módulo é o de aplicação das técnicas. A partir do código-fonte formatado e as configurações carregados pelo primeiro módulo, este módulo analisa cada instrução e gera as modificações necessárias.

III. Implementação

A CFT foi implementada em Java, devido ao seu suporte a modularidade, organização de código e análise de expressões regulares, usada para extrair partes do texto.

As configurações são organizadas em arquivos de texto, que descrevem os recursos do processador e suas permissões de leitura e escrita, além de informações sobre a execução do programa para gerar as alterações.

Ao fim do código, a CFT gera uma rotina de detecção de erro, que sinaliza o mesmo e interrompe a execução do programa.

IV. Conclusão

Este resumo apresentou a CFT, uma ferramenta capaz de proteger processadores contra erros causados por interferência externa.

A ferramenta implementa automaticamente uma série de técnicas de detecção baseadas em software no código-fonte de um programa.

A CFT é independente da arquitetura do processador, já que é configurada pelo usuário no momento da execução.